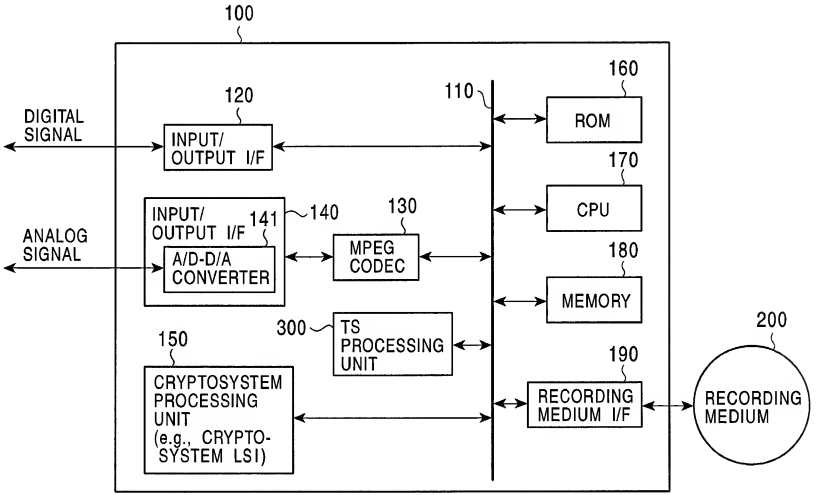
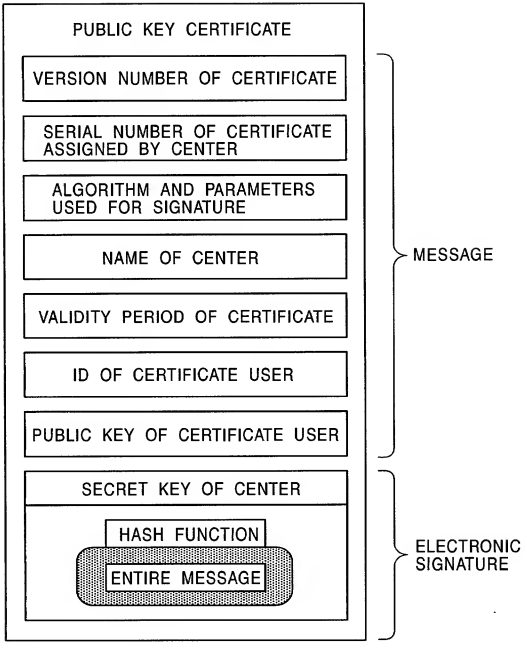
EP02015015.0215202

FIG. 1



502 of 02

FIG. 2



1005015-021202

FIG. 3A

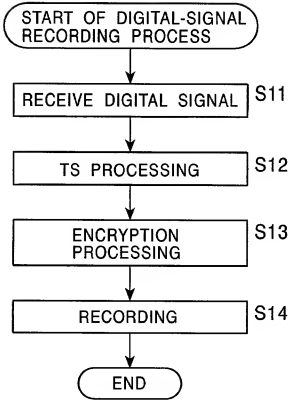
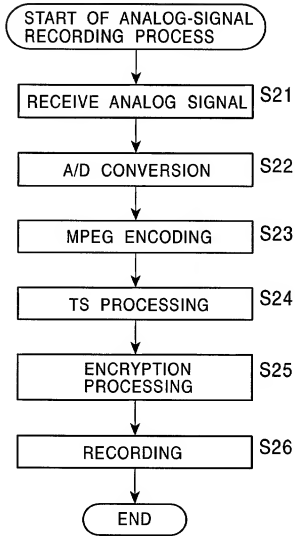


FIG. 3B



2020-505001

FIG. 4A

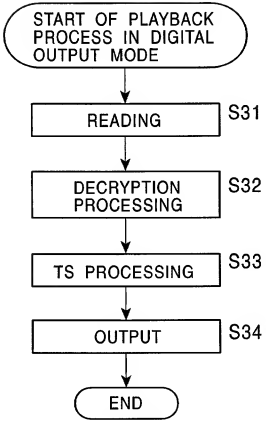
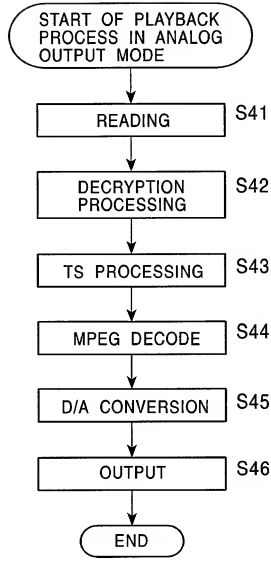


FIG. 4B



EP 2 271 090 A2 - 05-01-2011

2021.02.05 15:35:07 KIPO

FIG. 5

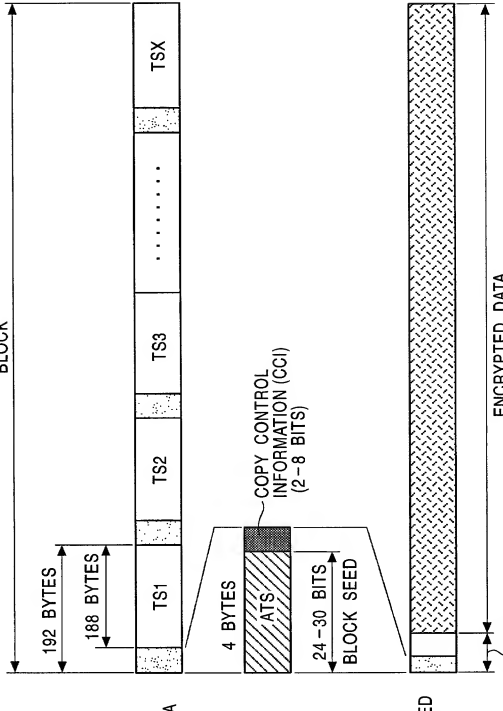


FIG. 6

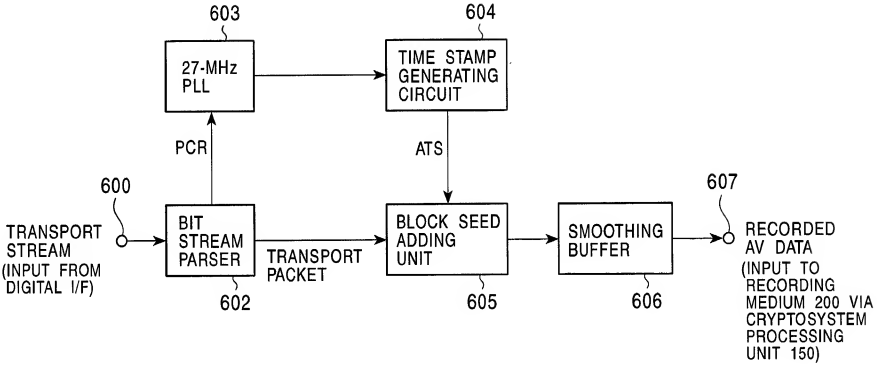

603
27-MHz PLL
604
TIME STAMP GENERATING CIRCUIT
PCR
ATS
600
607
TRANSPORT STREAM (INPUT FROM DIGITAL I/F)
BIT STREAM PARSER
TRANSPORT PACKET
BLOCK SEED ADDING UNIT
SMOOTHING BUFFER
RECORDED AV DATA (INPUT TO RECORDING MEDIUM 200 VIA CRYPTOSYSTEM PROCESSING UNIT 150)
602
605
606

FIG. 7A

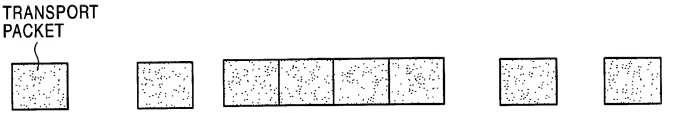


FIG. 7B

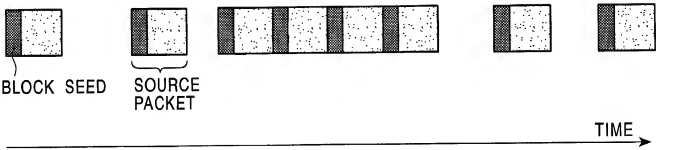


FIG. 7C

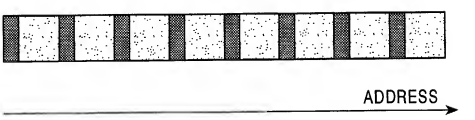


FIG. 8

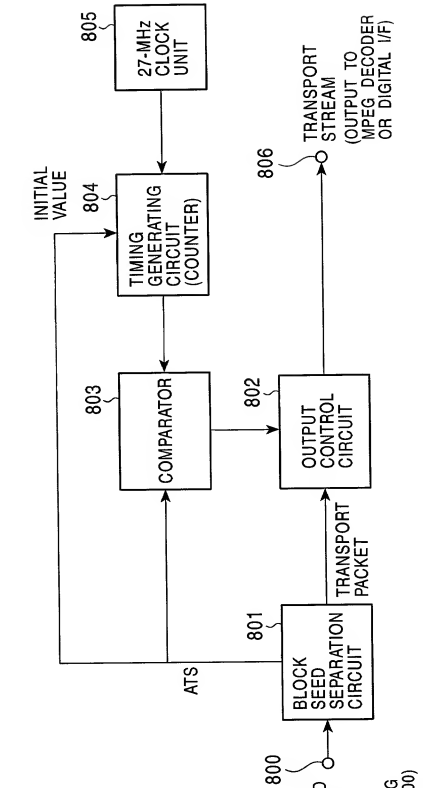
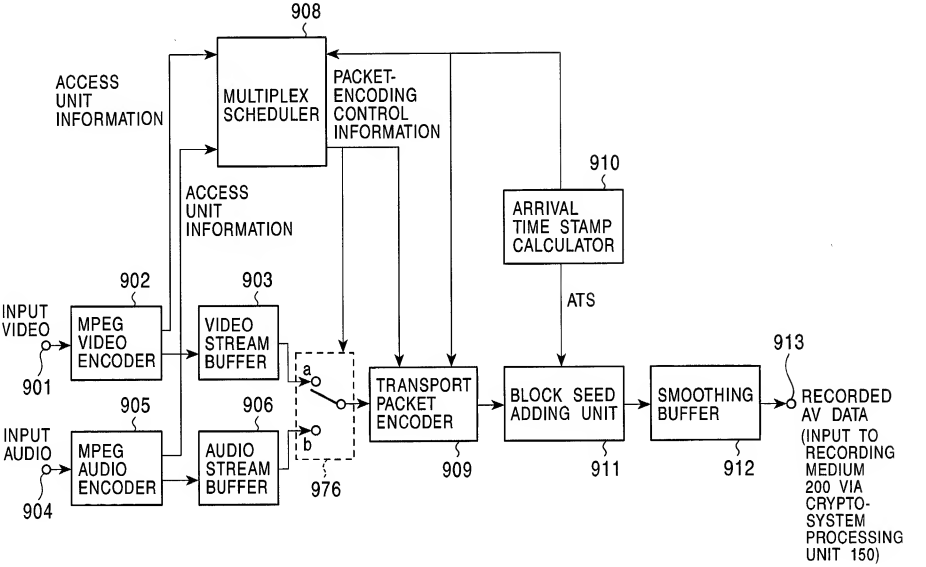

800
RECORDED AV DATA (SUPPLIED FROM RECORDING MEDIUM 200)
801
BLOCK SEED SEPARATION CIRCUIT
ATS
TRANSPORT PACKET
802
OUTPUT CONTROL CIRCUIT
803
COMPARATOR
804
TIMING GENERATING CIRCUIT (COUNTER)
INITIAL VALUE
805
27-MHz CLOCK UNIT
806
TRANSPORT STREAM (OUTPUT TO MPEG DECODER OR DIGITAL I/F)

FIG. 9


908
MULTIPLEX SCHEDULER
ACCESS UNIT INFORMATION
PACKET-ENCODING CONTROL INFORMATION
ACCESS UNIT INFORMATION
910
ARRIVAL TIME STAMP CALCULATOR
ATS
902
903
INPUT VIDEO
MPEG VIDEO ENCODER
VIDEO STREAM BUFFER
901
905
906
INPUT AUDIO
MPEG AUDIO ENCODER
AUDIO STREAM BUFFER
904
a
b
976
TRANSPORT PACKET ENCODER
909
BLOCK SEED ADDING UNIT
911
SMOOTHING BUFFER
912
913
RECORDED AV DATA
(INPUT TO RECORDING MEDIUM 200 VIA CRYPTO-SYSTEM PROCESSING UNIT 150)

EP1725015A1 '06-11-29

FIG. 10

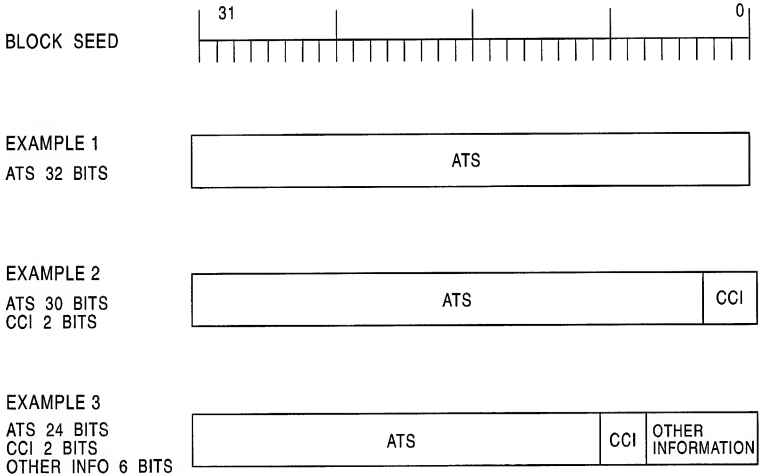


FIG. 11

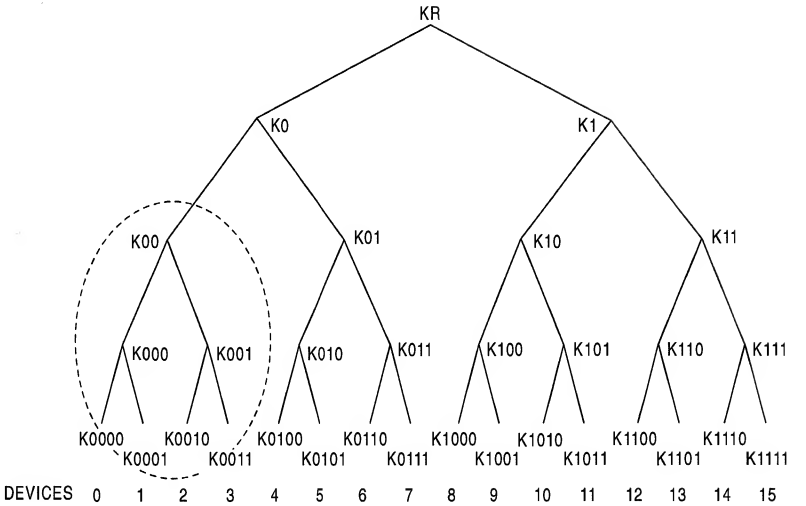

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
DEVICES 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

FIG. 12A

GENERATION: t	
INDEX	ENCRYPTION KEY
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

1007501S - 0234202

FIG. 12B

GENERATION: t	
INDEX	ENCRYPTION KEY
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG. 13

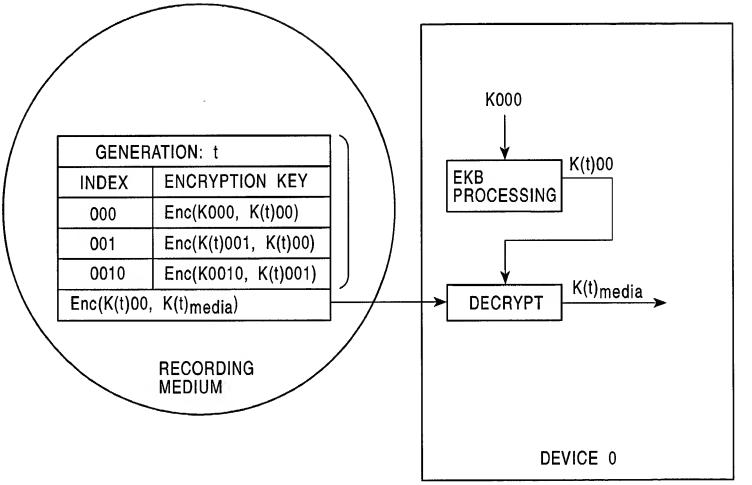

GENERATION: t
INDEX
ENCRYPTION KEY
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)media)
RECORDING MEDIUM
K000
EKB PROCESSING
K(t)00
DECRYPT
K(t)media
DEVICE 0

FIG. 14

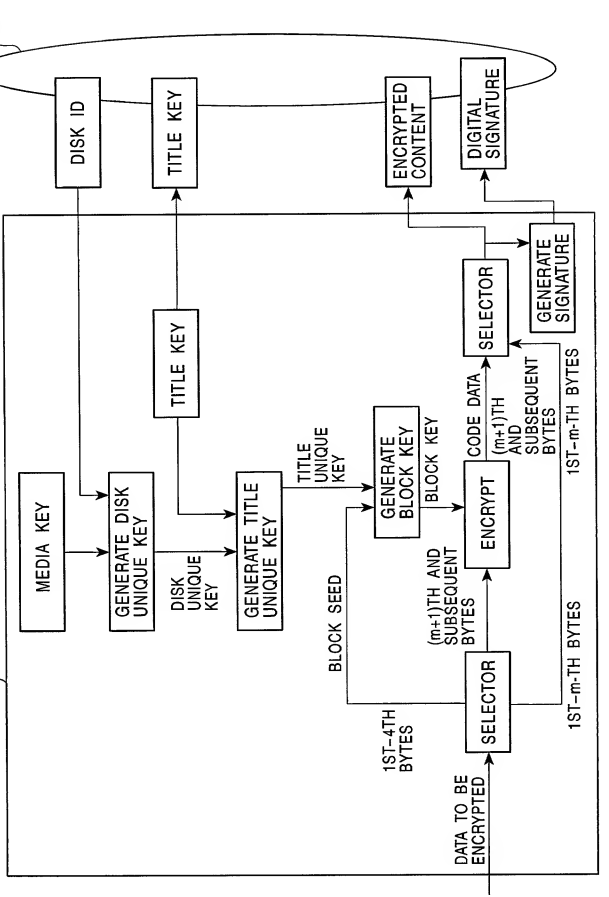

100
200
MEDIA KEY
GENERATE DISK UNIQUE KEY
DISK UNIQUE KEY
GENERATE TITLE UNIQUE KEY
TITLE UNIQUE KEY
GENERATE BLOCK KEY
BLOCK KEY
ENCRYPT
CODE DATA
SELECTOR
GENERATE SIGNATURE
DISK ID
TITLE KEY
ENCRYPTED CONTENT
DIGITAL SIGNATURE
TITLE KEY
BLOCK SEED
1ST-4TH BYTES
(m+1)TH AND SUBSEQUENT BYTES
(m+1)TH AND SUBSEQUENT BYTES
1ST-m-TH BYTES
1ST-m-TH BYTES
DATA TO BE ENCRYPTED
SELECTOR

FIG. 15A

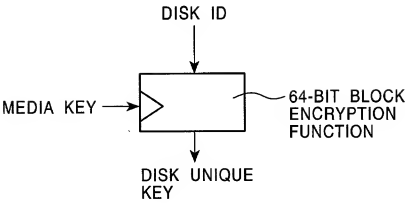
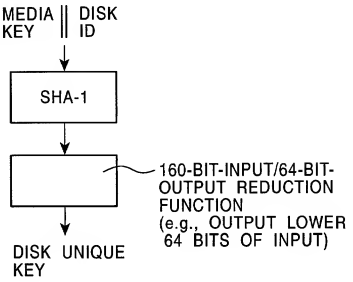


FIG. 15B



EP 1 507 265 A2 23.02.2005

FIG. 16A

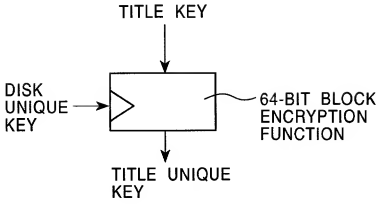
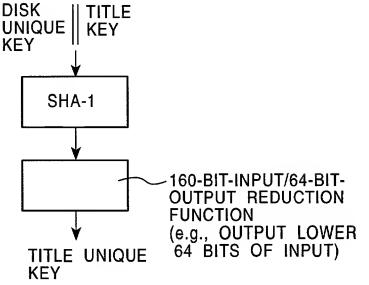


FIG. 16B



EP 1 605 451 A2 07.12.2005

FIG. 17A

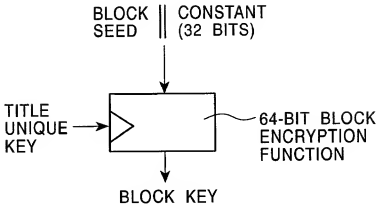
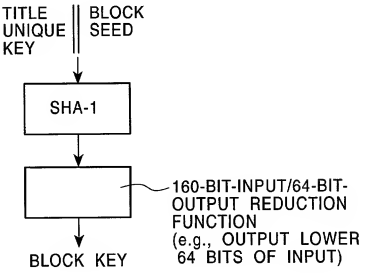
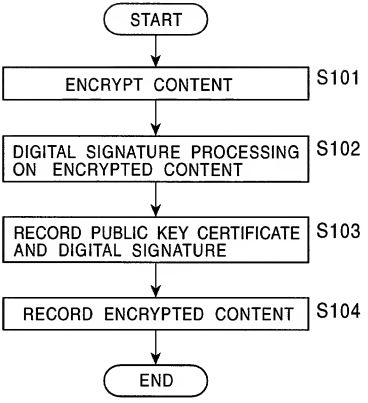


FIG. 17B



1007501S · 021202

FIG. 18



EP 2 071 569 A1 2009-06-17

FIG. 19

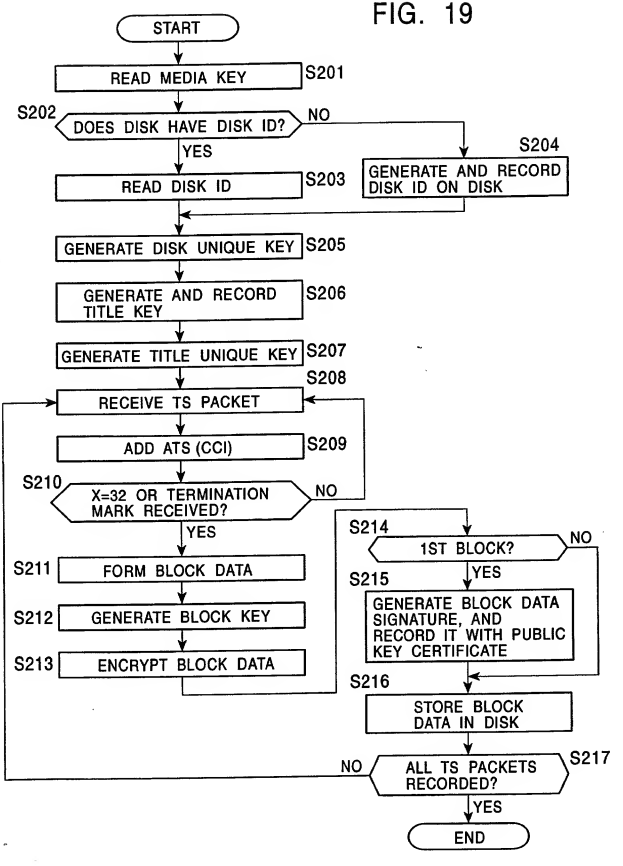
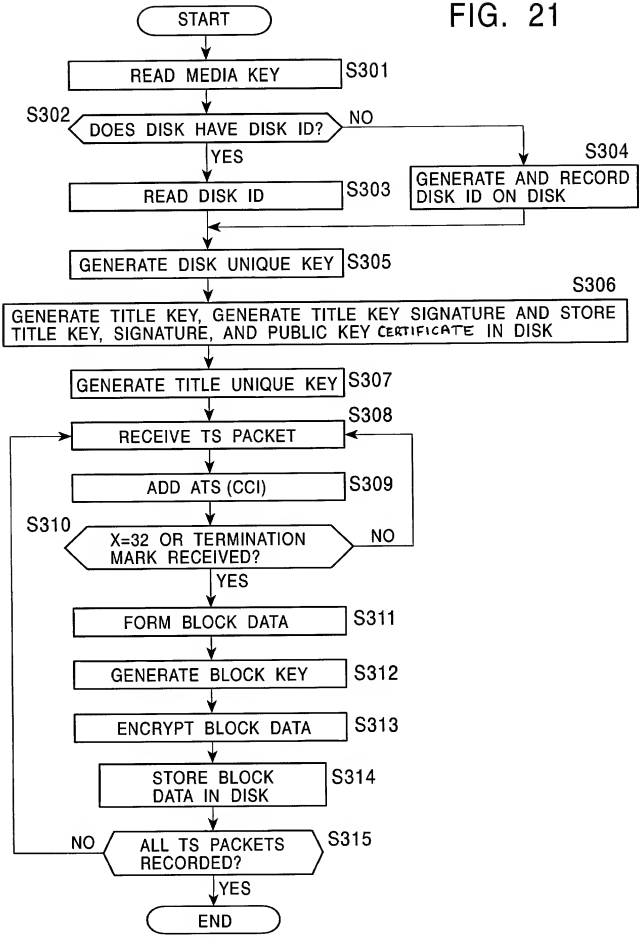

START
READ MEDIA KEY
S201
S202
DOES DISK HAVE DISK ID?
NO
YES
S204
GENERATE AND RECORD DISK ID ON DISK
READ DISK ID
S203
GENERATE DISK UNIQUE KEY
S205
GENERATE AND RECORD TITLE KEY
S206
GENERATE TITLE UNIQUE KEY
S207
S208
RECEIVE TS PACKET
ADD ATS (CCI)
S209
S210
X=32 OR TERMINATION MARK RECEIVED?
NO
YES
S211
FORM BLOCK DATA
S212
GENERATE BLOCK KEY
S213
ENCRYPT BLOCK DATA
S214
1ST BLOCK?
NO
YES
S215
GENERATE BLOCK DATA SIGNATURE, AND RECORD IT WITH PUBLIC KEY CERTIFICATE
S216
STORE BLOCK DATA IN DISK
S217
NO
ALL TS PACKETS RECORDED?
YES
END

FIG. 20

FILE 1	CONTENT DATA ADDRESS
	TITLE KEY ADDRESS
	DIGITAL SIGNATURE ADDRESS
	PUBLIC KEY CERTIFICATE ADDRESS
	OTHER INFORMATION
FILE 2	CONTENT DATA ADDRESS
	TITLE KEY ADDRESS
	DIGITAL SIGNATURE ADDRESS
	PUBLIC KEY CERTIFICATE ADDRESS
	OTHER INFORMATION
⋮	⋮

1007501S · 021202

FIG. 21



EP 2 071 570 A1 2009.06.17

FIG. 22

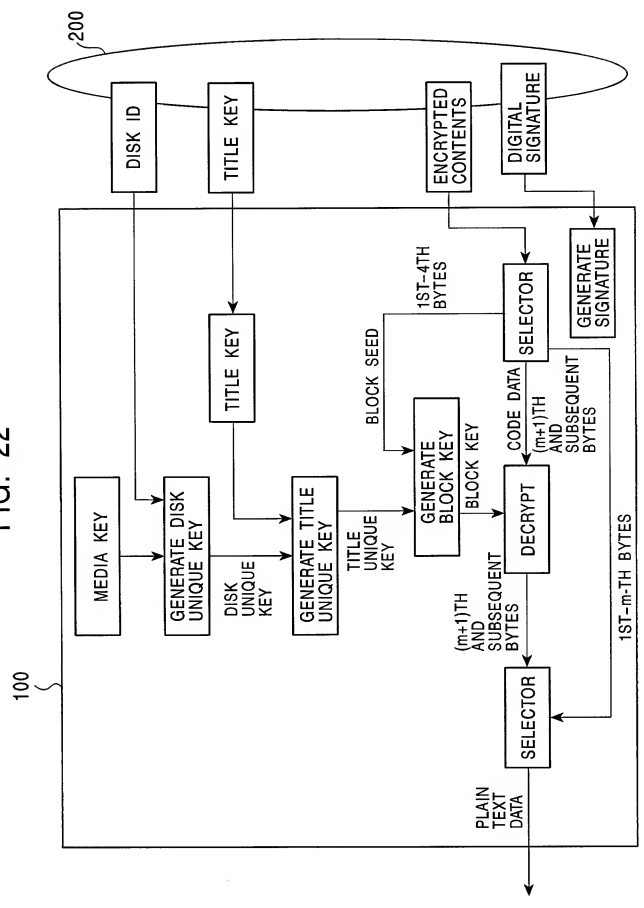
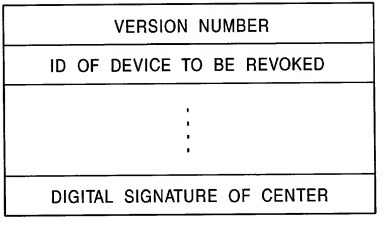

100
200
DISK ID
TITLE KEY
ENCRYPTED CONTENTS
DIGITAL SIGNATURE
MEDIA KEY
GENERATE DISK UNIQUE KEY
DISK UNIQUE KEY
GENERATE TITLE UNIQUE KEY
TITLE UNIQUE KEY
TITLE KEY
BLOCK SEED
GENERATE BLOCK KEY
BLOCK KEY
1ST-4TH BYTES
SELECTOR
GENERATE SIGNATURE
CODE DATA
(m+1)TH AND SUBSEQUENT BYTES
DECRYPT
(m+1)TH AND SUBSEQUENT BYTES
1ST-m-TH BYTES
SELECTOR
PLAIN TEXT DATA

FIG. 23



EP 1 705 855 A1 20061227

FIG. 24

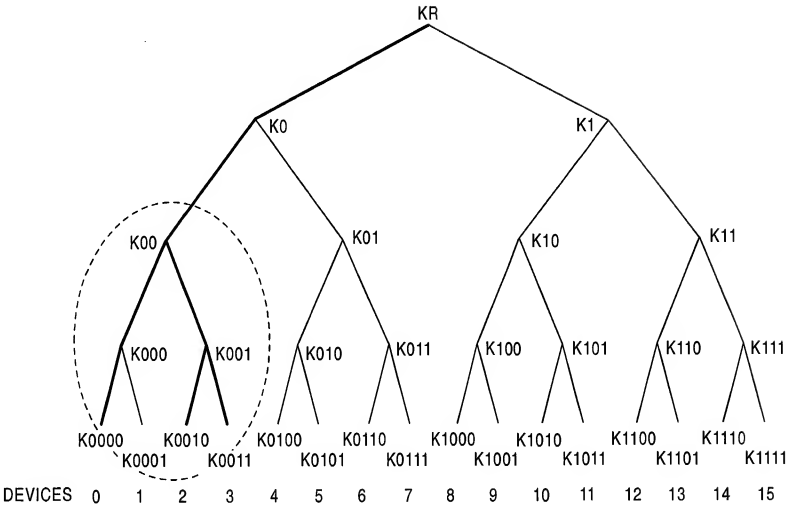
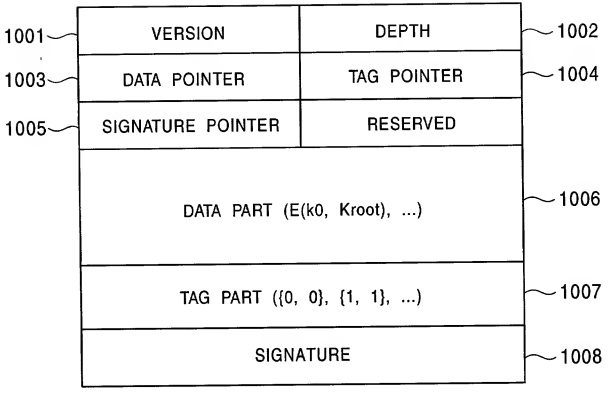

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
DEVICES 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

FIG. 25



1007150150-0220202

FIG. 26

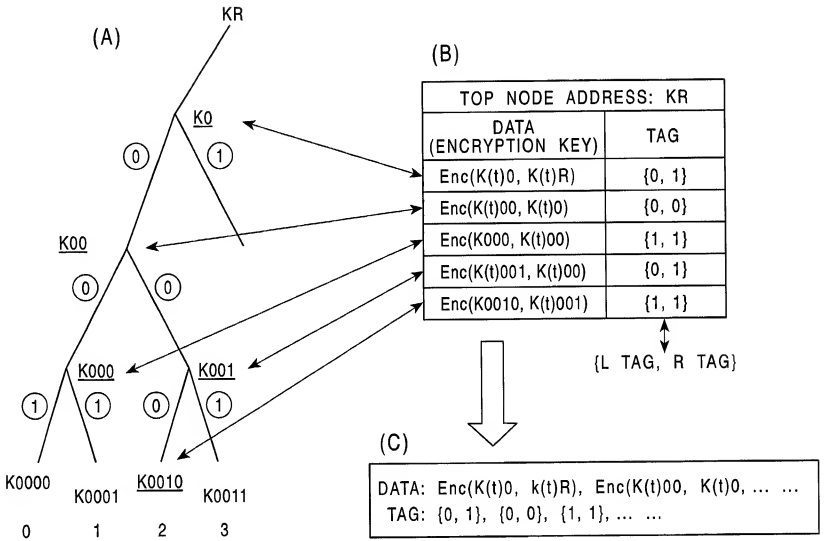

(A)
KR
K0
0
1
K00
0
0
K000
K001
1
1
0
1
K0000
K0001
K0010
K0011
0
1
2
3
(B)
TOP NODE ADDRESS: KR
DATA (ENCRYPTION KEY)
TAG
Enc(K(t)0, K(t)R)
{0, 1}
Enc(K(t)00, K(t)0)
{0, 0}
Enc(K000, K(t)00)
{1, 1}
Enc(K(t)001, K(t)00)
{0, 1}
Enc(K0010, K(t)001)
{1, 1}
{L TAG, R TAG}
(C)
DATA: Enc(K(t)0, k(t)R), Enc(K(t)00, K(t)0, ...
TAG: {0, 1}, {0, 0}, {1, 1}, ...

FIG. 27A

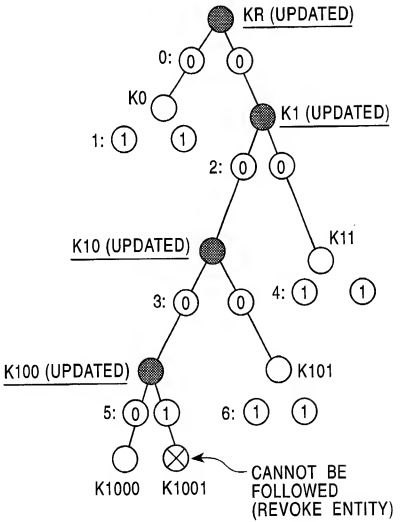


FIG. 27B

DATA (ENCRYPTION KEY)	Enc(K0, K(t)R), Enc(K(t)1, K(t)R) Enc(K(t)10, K(t)1), Enc(K11, K(t)1) Enc(K(t)100, K(t)10), Enc(K101, K(t)10) Enc(K1000, K(t)100)
TAG	0: {0, 0}, 1: {1, 1}, 2: {0, 0}, 3: {0, 0}, 4: {1, 1}, 5: {0, 1}, 6: {1, 1},

{L TAG, R TAG}

FIG. 28A

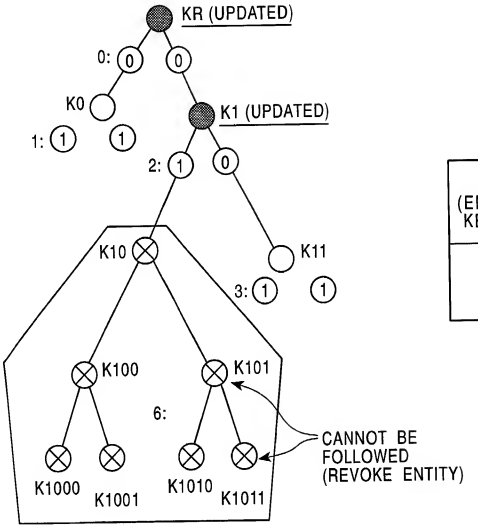


FIG. 28B

DATA (ENCRYPTION KEY)	Enc(K0, K(t)R), Enc(K(t)1, K(t)R) Enc(K11, K(t)1)
TAG	0: {0, 0}, 1: {1, 1}, 2: {1, 0}, 3: {1, 1}

{L TAG, R TAG}

FIG. 29

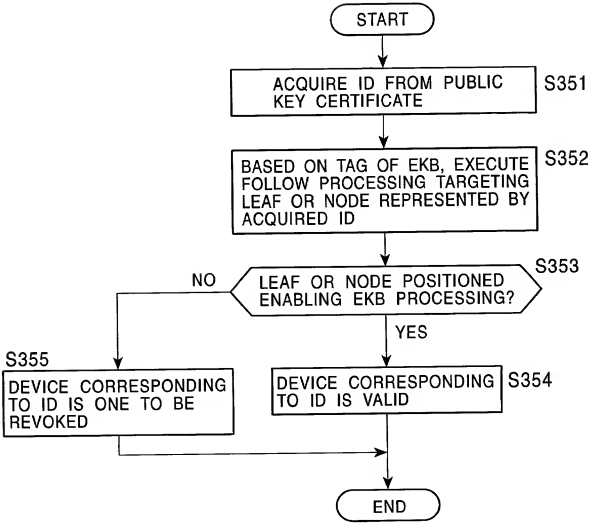
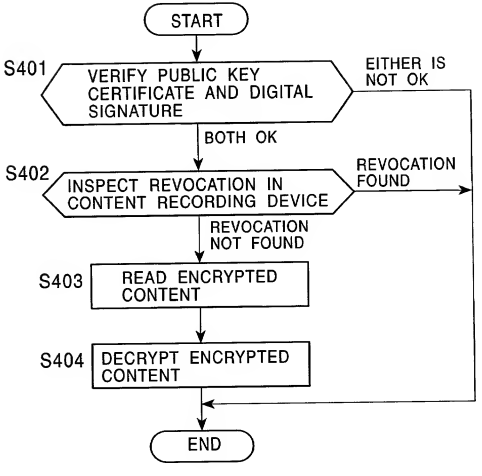

START
ACQUIRE ID FROM PUBLIC KEY CERTIFICATE
S351
BASED ON TAG OF EKB, EXECUTE FOLLOW PROCESSING TARGETING LEAF OR NODE REPRESENTED BY ACQUIRED ID
S352
LEAF OR NODE POSITIONED ENABLING EKB PROCESSING?
S353
NO
YES
DEVICE CORRESPONDING TO ID IS VALID
S354
DEVICE CORRESPONDING TO ID IS ONE TO BE REVOKED
S355
END

FIG. 30



EP 2 057 801 A1 2009-05-06

FIG. 31

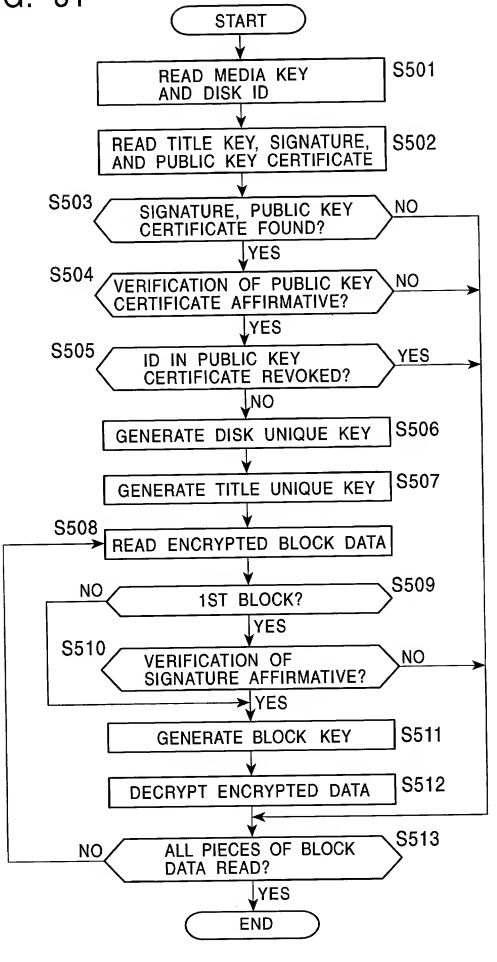
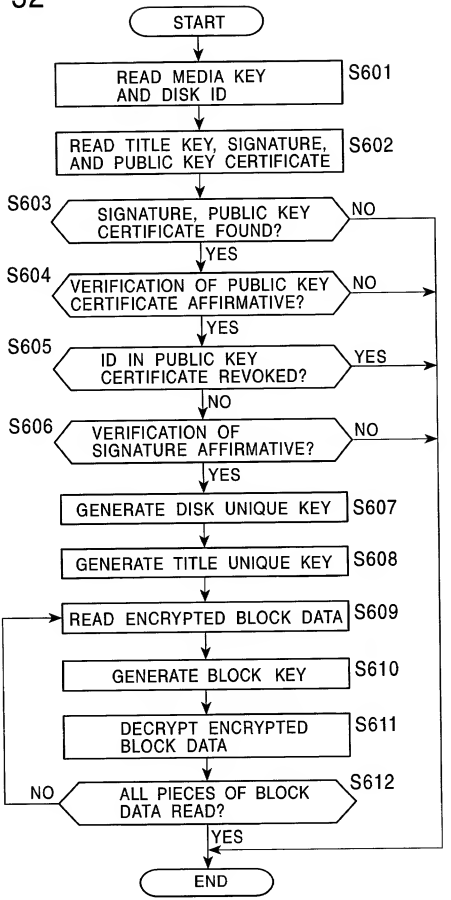

START
READ MEDIA KEY AND DISK ID
S501
READ TITLE KEY, SIGNATURE, AND PUBLIC KEY CERTIFICATE
S502
S503
SIGNATURE, PUBLIC KEY CERTIFICATE FOUND?
NO
YES
S504
VERIFICATION OF PUBLIC KEY CERTIFICATE AFFIRMATIVE?
NO
YES
S505
ID IN PUBLIC KEY CERTIFICATE REVOKED?
YES
NO
GENERATE DISK UNIQUE KEY
S506
GENERATE TITLE UNIQUE KEY
S507
S508
READ ENCRYPTED BLOCK DATA
NO
1ST BLOCK?
S509
YES
S510
VERIFICATION OF SIGNATURE AFFIRMATIVE?
NO
YES
GENERATE BLOCK KEY
S511
DECRYPT ENCRYPTED DATA
S512
NO
ALL PIECES OF BLOCK DATA READ?
S513
YES
END

FIG. 32



2024-20-54-057-1007-EP-1

FIG. 33A

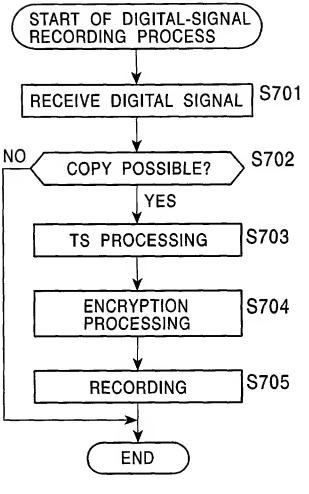
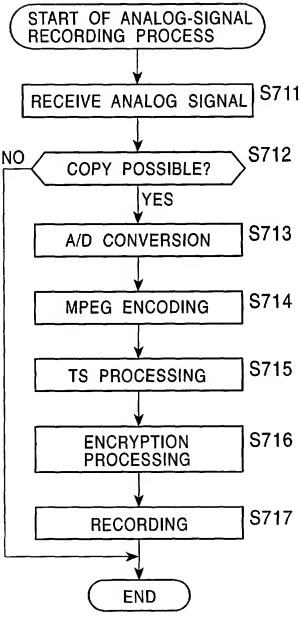


FIG. 33B



2021.20.5105.2001

FIG. 34A

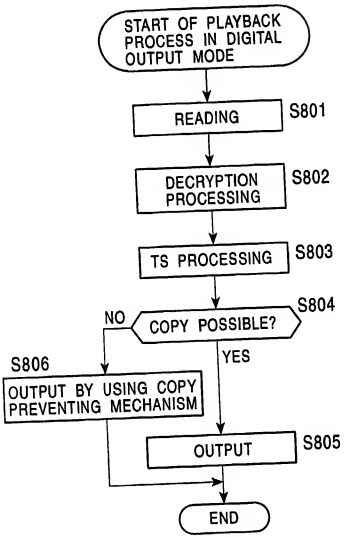


FIG. 34B

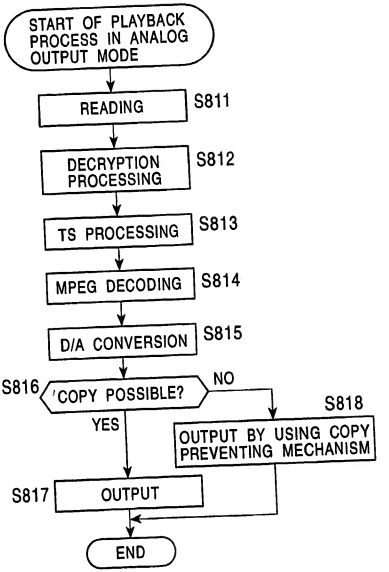
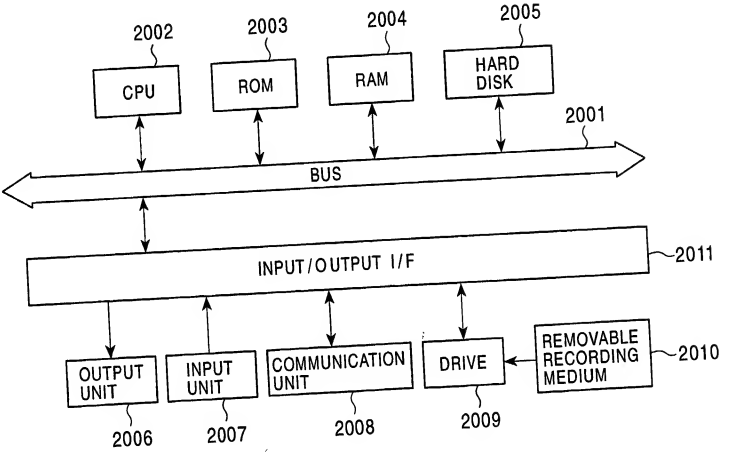


FIG. 35


2002
2003
2004
2005
CPU
ROM
RAM
HARD DISK
2001
BUS
INPUT/OUTPUT I/F
2011
OUTPUT UNIT
INPUT UNIT
COMMUNICATION UNIT
DRIVE
REMOVABLE RECORDING MEDIUM
2010
2006
2007
2008
2009